U.S. Department of Justice

Federal Bureau of Investigation
Washington, D.C. 20535

August 21, 2019

MUCK ROCK NEWS
411A HIGHLAND AVENUE
DEPT MR 62138
SOMERVILLE, MA 02144

FOIPA Request No.: 1428805-000
Subject: Contract # DJF171200P0005393

Dear Mr. Richards:

The enclosed documents were reviewed under the Freedom of Information/Privacy Acts (FOIPA), Title 5, United States Code, Section 552/552a. Below you will find check boxes under the appropriate statute headings which indicate the types of exemptions asserted to protect information which is exempt from disclosure. The appropriate exemptions are noted on the enclosed pages next to redacted information. In addition, a deleted page information sheet was inserted to indicate where pages were withheld entirely and identify which exemptions were applied. The checked exemption boxes used to withhold information are further explained in the enclosed Explanation of Exemptions.

Section 552		Section 552a
☐ (b)(1)	☐ (b)(7)(A)	☐ (d)(5)
☐ (b)(2)	☐ (b)(7)(B)	☐ (j)(2)
☐ (b)(3)	☑ (b)(7)(C)	☐ (k)(1)
_____	☐ (b)(7)(D)	☐ (k)(2)
_____	☑ (b)(7)(E)	☐ (k)(3)
_____	☐ (b)(7)(F)	☐ (k)(4)
☑ (b)(4)	☐ (b)(8)	☐ (k)(5)
☐ (b)(5)	☐ (b)(9)	☐ (k)(6)
☑ (b)(6)		☐ (k)(7)

13 page(s) were reviewed and 10 page(s) are being released.

Please see the paragraphs below for relevant information specific to your request as well as the enclosed FBI FOIPA Addendum for standard responses applicable to all requests.

☐ Document(s) were located which originated with, or contained information concerning, other Government Agency (ies) [OGA].

☐ This information has been referred to the OGA(s) for review and direct response to you.
☐ We are consulting with another agency. The FBI will correspond with you regarding this information when the consultation is completed.

Please refer to the enclosed FBI FOIPA Addendum for additional standard responses applicable to your request. **"Part 1"** of the Addendum includes standard responses that apply to all requests. **"Part 2"** includes additional standard responses that apply to all requests for records on individuals. **"Part 3"** includes general information about FBI records that you may find useful. Also enclosed is our Explanation of Exemptions.

For questions regarding our determinations, visit the www.fbi.gov/foia website under "Contact Us."

The FOIPA Request Number listed above has been assigned to your request. Please use this number in all correspondence concerning your request.

You may file an appeal by writing to the Director, Office of Information Policy (OIP), United States Department of Justice, Suite 11050, 1425 New York Avenue, NW, Washington, D.C. 20530-0001, or you may submit an appeal through OIP's FOIA online portal by creating an account on the following website: https://www.foiaonline.gov/foiaonline/action/public/home. Your appeal must be postmarked or electronically transmitted within ninety (90) days from the date of this letter in order to be considered timely. If you submit your appeal by mail, both the letter and the envelope should be clearly marked "Freedom of Information Act Appeal." Please cite the FOIPA Request Number assigned to your request so it may be easily identified.

You may seek dispute resolution services by contacting the Office of Government Information Services (OGIS) at 877-684-6448, or by emailing ogis@nara.gov. Alternatively, you may contact the FBI's FOIA Public Liaison by emailing foipaquestions@fbi.gov. If you submit your dispute resolution correspondence by email, the subject heading should clearly state "Dispute Resolution Services." Please also cite the FOIPA Request Number assigned to your request so it may be easily identified.

☑ See additional information which follows.

Sincerely,

David M. Hardy
Section Chief
Record/Information
Dissemination Section
Information Management Division

Enclosure(s)

The enclosed documents represent the final release of information responsive to your FOIPA request. This material is being provided to you at no charge.

FBI FOIPA Addendum

As referenced in our letter responding to your Freedom of Information/Privacy Acts (FOIPA) request, the FBI FOIPA Addendum includes information applicable to your request. Part 1 of the Addendum includes standard responses that apply to all requests. Part 2 includes additional standard responses that apply to all requests for records on individuals. Part 3 includes general information about FBI records. For questions regarding Parts 1, 2, or 3, visit the www.fbi.gov/foia website under "Contact Us." Previously mentioned appeal and dispute resolution services are also available at the web address.

Part 1: The standard responses below apply to all requests:

(i) **5 U.S.C. § 552(c).** Congress excluded three categories of law enforcement and national security records from the requirements of the FOIA [5 U.S.C. § 552(c) (2006 & Supp. IV (2010)]. FBI responses are limited to those records subject to the requirements of the FOIA. Additional information about the FBI and the FOIPA can be found on the www.fbi.gov/foia website.

(ii) **National Security/Intelligence Records.** The FBI can neither confirm nor deny the existence of national security and foreign intelligence records pursuant to FOIA exemptions (b)(1), (b)(3), and PA exemption (j)(2) as applicable to requests for records about individuals [5 U.S.C. §§ 552/552a (b)(1), (b)(3), and (j)(2); 50 U.S.C § 3024(i)(1)]. The mere acknowledgment of the existence or nonexistence of such records is itself a classified fact protected by FOIA exemption (b)(1) and/or would reveal intelligence sources, methods, or activities protected by exemption (b)(3) [50 USC § 3024(i)(1)]. This is a standard response and should not be read to indicate that national security or foreign intelligence records do or do not exist.

Part 2: The standard responses below apply to all requests for records on individuals:

(i) **Requests for Records about any Individual—Watch Lists.** The FBI can neither confirm nor deny the existence of any individual's name on a watch list pursuant to FOIA exemption (b)(7)(E) and PA exemption (j)(2) [5 U.S.C. §§ 552/552a (b)(7)(E), (j)(2)]. This is a standard response and should not be read to indicate that watch list records do or do not exist.

(ii) **Requests for Records for Incarcerated Individuals.** The FBI can neither confirm nor deny the existence of records which could reasonably be expected to endanger the life or physical safety of any incarcerated individual pursuant to FOIA exemptions (b)(7)(E), (b)(7)(F), and PA exemption (j)(2) [5 U.S.C. §§ 552/552a (b)(7)(E), (b)(7)(F), and (j)(2)]. This is a standard response and should not be read to indicate that such records do or do not exist.

Part 3: General Information:

(i) **Record Searches.** The Record/Information Dissemination Section (RIDS) searches for reasonably described records by searching those systems or locations where responsive records would reasonably be found. Most requests are satisfied by searching the Central Records System (CRS), an extensive system of records consisting of applicant, investigative, intelligence, personnel, administrative, and general files compiled and maintained by the FBI in the course of fulfilling its dual law enforcement and intelligence mission as well as the performance of agency administrative and personnel functions. The CRS spans the entire FBI organization and encompasses the records of FBI Headquarters (FBIHQ), FBI Field Offices, and FBI Legal Attaché Offices (Legats) worldwide. A CRS search includes Electronic Surveillance (ELSUR) records.

(ii) **FBI Records.** Founded in 1908, the FBI carries out a dual law enforcement and national security mission. As part of this dual mission, the FBI creates and maintains records on various subjects; however, the FBI does not maintain records on every person, subject, or entity.

(iii) **Requests for Criminal History Records or Rap Sheets.** The Criminal Justice Information Services (CJIS) Division provides Identity History Summary Checks – often referred to as a criminal history record or rap sheets. These criminal history records are not the same as material in an investigative "FBI file." An Identity History Summary Check is a listing of information taken from fingerprint cards and documents submitted to the FBI in connection with arrests, federal employment, naturalization, or military service. For a fee, individuals can request a copy of their Identity History Summary Check. Forms and directions can be accessed at www.fbi.gov/about-us/cjis/identity-history-summary-checks. Additionally, requests can be submitted electronically at www.edo.cjis.gov. For additional information, please contact CJIS directly at (304) 625-5590.

(iv) **The National Name Check Program (NNCP).** The mission of NNCP is to analyze and report information in response to name check requests received from federal agencies, for the purpose of protecting the United States from foreign and domestic threats to national security. Please be advised that this is a service provided to other federal agencies. Private citizens cannot request a name check.

EXPLANATION OF EXEMPTIONS

SUBSECTIONS OF TITLE 5, UNITED STATES CODE, SECTION 552

(b)(1) (A) specifically authorized under criteria established by an Executive order to be kept secret in the interest of national defense or foreign policy and (B) are in fact properly classified to such Executive order;

(b)(2) related solely to the internal personnel rules and practices of an agency;

(b)(3) specifically exempted from disclosure by statute (other than section 552b of this title), provided that such statute (A) requires that the matters be withheld from the public in such a manner as to leave no discretion on issue, or (B) establishes particular criteria for withholding or refers to particular types of matters to be withheld;

(b)(4) trade secrets and commercial or financial information obtained from a person and privileged or confidential;

(b)(5) inter-agency or intra-agency memorandums or letters which would not be available by law to a party other than an agency in litigation with the agency;

(b)(6) personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy;

(b)(7) records or information compiled for law enforcement purposes, but only to the extent that the production of such law enforcement records or information (A) could reasonably be expected to interfere with enforcement proceedings, (B) would deprive a person of a right to a fair trial or an impartial adjudication, (C) could reasonably be expected to constitute an unwarranted invasion of personal privacy, (D) could reasonably be expected to disclose the identity of confidential source, including a State, local, or foreign agency or authority or any private institution which furnished information on a confidential basis, and, in the case of record or information compiled by a criminal law enforcement authority in the course of a criminal investigation, or by an agency conducting a lawful national security intelligence investigation, information furnished by a confidential source, (E) would disclose techniques and procedures for law enforcement investigations or prosecutions, or would disclose guidelines for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk circumvention of the law, or (F) could reasonably be expected to endanger the life or physical safety of any individual;

(b)(8) contained in or related to examination, operating, or condition reports prepared by, on behalf of, or for the use of an agency responsible for the regulation or supervision of financial institutions; or

(b)(9) geological and geophysical information and data, including maps, concerning wells.

SUBSECTIONS OF TITLE 5, UNITED STATES CODE, SECTION 552a

(d)(5) information compiled in reasonable anticipation of a civil action proceeding;

(j)(2) material reporting investigative efforts pertaining to the enforcement of criminal law including efforts to prevent, control, or reduce crime or apprehend criminals;

(k)(1) information which is currently and properly classified pursuant to an Executive order in the interest of the national defense or foreign policy, for example, information involving intelligence sources or methods;

(k)(2) investigatory material compiled for law enforcement purposes, other than criminal, which did not result in loss of a right, benefit or privilege under Federal programs, or which would identify a source who furnished information pursuant to a promise that his/her identity would be held in confidence;

(k)(3) material maintained in connection with providing protective services to the President of the United States or any other individual pursuant to the authority of Title 18, United States Code, Section 3056;

(k)(4) required by statute to be maintained and used solely as statistical records;

(k)(5) investigatory material compiled solely for the purpose of determining suitability, eligibility, or qualifications for Federal civilian employment or for access to classified information, the disclosure of which would reveal the identity of the person who furnished information pursuant to a promise that his/her identity would be held in confidence;

(k)(6) testing or examination material used to determine individual qualifications for appointment or promotion in Federal Government service the release of which would compromise the testing or examination process;

(k)(7) material used to determine potential for promotion in the armed services, the disclosure of which would reveal the identity of the person who furnished the material pursuant to a promise that his/her identity would be held in confidence.

FEDERAL BUREAU OF INVESTIGATION
FOI/PA
DELETED PAGE INFORMATION SHEET
FOI/PA# 1428805-0

Total Deleted Page(s) = 3
Page 1 ~ b4; b6; b7C; b7E;
Page 3 ~ b4; b6; b7C; b7E;
Page 4 ~ b4; b6; b7C; b7E;

XXXXXXXXXXXXXXXXXXXXXXX
X Deleted Page(s) X
X No Duplication Fee X
X For this Page X
XXXXXXXXXXXXXXXXXXXXXXX

FD-369 (Rev. 08-13-12)

FEDERAL BUREAU OF INVESTIGATION

REQUISITION FOR GOODS AND SERVICES

DJF-17-3790-PR-0008391
Req.#

05/31/2017
Date

[redacted] 3790
Ordering Office/Cost Code

[redacted] (FBI)
Approved By

[redacted] (FBI)
Funding Approved By:

b6
b7C
b7E

CONTACT INFORMATION:

[redacted]

CLOSE-OUT INFORMATION:

Contract Specialist:
Date Received:
Purchase Order #:
Date Completed:

b6
b7C

LINE#	FULL DESCRIPTION	UNIT OF MEASURE	QTY	FUND CODE	PROGRAM/ SUBPROGRAM	SOC	SSOC	ORG 2	ORG 4	BBFY	EBFY	AGREEMENT #	AGREEMENT LINE #	POP BEG	POP END	DEL CODE	UNIT PRICE	EXTENDED AMOUNT
0001	[redacted]	[redacted]	[redacted]	SED1	L/2/ 4T	25218		0500	3790	2017				06/26/2017	09/30/2017	3790 3790	[redacted]	b4 b7E

TOTAL $4,995.00

ADDITIONAL INFORMATION:

Required Date:
Fiscal Year: FY17
Delivery Restrictions:
New Requirement (Yes/No):
Previous PO # / Contract #:
Exercising an Option on an Existing Contract: [redacted]

Government Estimate: [redacted]
Current Contract Year:
Estimated Funding Year 1:
Estimated Funding Year 2:
Estimated Funding Year 3:
Estimated Funding Year 4:

b4
b7E

FD-369a (Rev. 08-13-12)

FEDERAL BUREAU OF INVESTIGATION

REQUISITION FOR GOODS AND SERVICES

DJF-17-3790-PR-0008391
Req.#

05/31/2017
Date

[redacted]3790
Ordering Office/Cost Code

[redacted](FBI)
Approved By

[redacted](FBI)
Funding Approved By:

b6
b7C
b4
b7E

Acquisition Plan Number:

Estimated Funding Year 5: [redacted]

Suggested Vendor: HAWK ANALYTICS - DUNS No. 079871272

Contract Vehicle:

ORDER FOR SUPPLIES OR SERVICES

IMPORTANT: Mark all packages and papers with contract and/or order numbers.

1. DATE OF ORDER	2. CONTRACT NO. *(If any)*
06/21/2017	
3. ORDER NO.	**4. REQUISITION/REFERENCE NO.**
DJF-17-1200-P-0005393	DJF-17-3790-PR-0008391

5. ISSUING OFFICE *(Address correspondence to)*
FEDERAL BUREAU OF INVESTIGATION
PROCUREMENT SECTION
935 PENNSYLVANIA AVE. NW
ROOM 6823
WASHINGTON, DC 20535-0001

6. SHIP TO:
a. NAME OF CONSIGNEE
SEE SCHEDULE
b. STREET ADDRESS
c. CITY | d. STATE | e. ZIP CODE
f. SHIP VIA

7. TO:
a. NAME OF CONTRACTOR
HAWK ANALYTICS, INC.
b. COMPANY NAME
DUNS: 079871272
c. STREET ADDRESS
2652 FM 407, SUITE 215-E
d. CITY: BARTONVILLE | e. STATE: TX | f. ZIP CODE: 76226-7024

8. TYPE OF ORDER
[X] a. PURCHASE
REFERENCE YOUR: _____
Please furnish the following on the terms and conditions specified on both sides of this order and on the attached sheet, if any, including delivery as indicated.
[ ] b. DELIVERY -- Except for billing instructions on the reverse, this delivery order is subject to instructions contained on this side only of this form and is issued subject to the terms and conditions of the above-numbered contract.

10. REQUISITIONING OFFICE

b6
b7C
b7E

9. ACCOUNTING AND APPROPRIATION DATA
FBI-2017-SED1-0600-3790-U2-4T-25218-2017

11. BUSINESS CLASSIFICATION *(Check appropriate box(es))*
[ ] a. SMALL [ ] b. OTHER THAN SMALL [ ] c. DISADVANTAGED [X] d. WOMEN-OWNED [ ] e. HUBZone
[ ] f. SERVICE-DISABLED VETERAN-OWNED [X] g. WOMEN-OWNED SMALL BUSINESS (WOSB) ELIGIBLE UNDER THE WOSB PROGRAM [ ] h. EDWOSB

12. F.O.B. POINT

13. PLACE OF		14. GOVERNMENT B/L NO.	15. DELIVER TO F.O.B. POINT ON OR BEFORE *(Date)*	16. DISCOUNT TERMS
a. INSPECTION	b. ACCEPTANCE			NET 30

17. SCHEDULE *(See reverse for Rejections)*

ITEM NO. (a)	SUPPLIES OR SERVICES (b)	QUANTITY ORDERED (c)	UNIT (d)	UNIT PRICE (e)	AMOUNT (f)	QUANTITY ACCEPTED (g)
0001	CELLHAWK SUBSCRIPTION					
	See Continuation Sheet(s)					

b4
b7E

18. SHIPPING POINT	19. GROSS SHIPPING WEIGHT	20. INVOICE NO.	17(h) TOT. *(Cont. pages)*

SEE BILLING INSTRUCTIONS ON REVERSE

21. MAIL INVOICE TO:
a. NAME
SUBMIT ALL INVOICES VIA EMAIL TO
b. STREET ADDRESS *(or P.O. Box)*
c. CITY | d. STATE | e. ZIP CODE

b4
b7E

17(i) GRAND TOTAL: $4,995.00

22. UNITED STATES OF AMERICA BY *(Signature)*

23. NAME *(Typed)*
Jenny M. Knight
TITLE: CONTRACTING/ORDERING OFFICER

b6
b7C

AUTHORIZED FOR LOCAL REPRODUCTION
PREVIOUS EDITION NOT USABLE

OPTIONAL FORM 347 (REV. 2/2012)
Prescribed by GSA/FAR 48 CFR 53.213(f)

Section 2 - Commodity or Services Schedule

SCHEDULE OF SUPPLIES/SERVICES

CONTINUATION SHEET

ITEM NO.	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
	Line Period of Performance: 06/21/2017 - 06/20/2018 Base Period **Delivery Schedule:** Quantity: 1.000000 FOB: Delivery Address:				

b4
b7E

Base Total:	
Exercised Options Total:	
Unexercised Options Total:	
Base and Options Total:	

FUNDING DETAILS:

ITEM NO.	FUNDING LINE	OBLIGATED AMOUNT	ACCOUNTING CODES
0001	1		2017 - SED1 - 0600 - 3790 - U2 - - - 25218 - - - - - - b4 b7E
		TOTAL: $4,995.00	

Section 3 - Contract Clauses

Clauses By Reference

52.252-2 CLAUSES INCORPORATED BY REFERENCE (FEB 1998)	
This contract incorporates one or more clauses by reference, with the same force and effect as if they were given in full text. Upon request, the Contracting Officer will make their full text available. Also, the full text of a clause may be accessed electronically at this/these address(es): www.acquisition.gov	
Clause	Title
52.212-4	Contract Terms and Conditions--Commercial Items (May 2015)
52.224-3	Privacy Training (Jan 2017)
52.224-3 Alt I	Privacy Training (Jan 2017) - Alternate I (Jan 2017)
52.232-39	Unenforceability of Unauthorized Obligations (Jun 2013)
52.232-40	Providing Accelerated Payments to Small Business Subcontractors (Dec 2013)

Clauses By Full Text

DJAR-PGD-02-02A Non-U.S. Citizens Prohibited from Access to DOJ Information Technology (IT) Systems

The Department of Justice does not permit the use of Non-U.S. citizens in the performance of this contract or commitment for any position that involves access to or development of any DOJ IT system. By signing the contract or commitment document, the contractor agrees to this restriction. [In those instances where other non-IT requirements contained in the contract or commitment can be met by using Non-U.S. citizens, those requirements shall be clearly described.].
(End of Clause)

DJAR-PGD-02-02B Non-U.S. Citizens Prohibited from Access to DOJ Information Technology (IT) Systems

The Department of Justice (DOJ) will no longer permit the use of Non-U.S. citizens in the performance of this contract or commitment for any position that involves access to or development of any DOJ IT system. By signing the contract or commitment document, the contractor agrees to this restriction with respect to all new employees utilized directly to perform duties on the contract. Non-U.S. citizens currently employees under this contract or commitment may continue performance unless otherwise directed by the Department of Justice. No new, replacement, or additional Non-U.S. citizens may be added to the contract without the express approval of the Department of Justice. [In those instances where other non-IT requirements contained in the contract or commitment can be met by using Non-U.S. citizens, those requirements shall be clearly described.].
(End of Clause)

DJAR-PGD-05-08 Implementation of Homeland Security Presidential Directive (HSPD) 12 - Policy for a Common Identification Standard for Federal Employees and Contractor

NOTICE OF CONTRACTOR PERSONNEL SECURITY REQUIREMENTS
Compliance with Homeland Security Presidential Directive-12 (HSPD-12) and Federal Information Processing Standard Publication 201 (FIPS 201)' entitled "Personal Identification Verification (PIV) for Federal Employees and Contractors," Phase I.

1. Long-Term Contractor Personnel:

In order to be compliant with HSPD-12/PIV I, the following investigative requirements must be met for each new long-term2 contractor employee whose background investigation (BI) process begins on or after October 27, 2005:

a. Contractor Personnel must present two forms of identification in original form prior to badge issuance (acceptable documents are listed in Form 1-9, OMB No. 1615-0047, " Employment Eligibility Verification," and at least one document must be a valid State or Federal government-issued picture ID);
b. Contractor Personnel must appear in person at least once before a DOJ official who is responsible for checking the identification documents. This identity proofing must be completed sometime during the clearance process but prior to badge issuance and must be documented by the DOJ official;
c. Contractor Personnel must undergo a BI commensurate with the designated risk level associated with the duties of each position. Outlined below are the minimum BI requirements for each risk level:
•High Risk - Background Investigation (5 year scope)
•Moderate Risk - Limited Background Investigation (LBI) or Minimum Background Investigation (MBI)
•Low Risk - National Agency Check with Inquiries (NACI) investigation
d. The pre-appointment BI waiver requirements for all position sensitivity levels are a:
1) Favorable review of the security questionnaire form;
2) Favorable fingerprint results;
3) Favorable credit report, if required;3
4) Waiver request memorandum, including both the Office of Personnel
Management schedule date and position sensitivity/risk level; and 5) Favorable review of the National Agency Check (NAC)4 portion of the applicable BI that is determined by position sensitivity/risk level.
A badge may be issued following approval of the above waiver requirements.
If the NAC is not received within five days of OPM' s scheduling date, the badge can be issued based on a favorable review of the Security Questionnaire and the Federal Bureau of Investigation Criminal History Check (i.e., fingerprint check results).
e. Badge re-validation will occur once the investigation is completed and favorably adjudicated. If the BI results so justify, badges issued under these procedures will be suspended or revoked.

2. Short-Term Contractor Personnel:
It is the policy of the DOJ that short-term contractors having access to DOJ information systems and/or DOJ facilities or space for six months or fewer are subject to the identity proofing requirements listed in items Ia. and Ib. above. The pre-appointment waiver requirements for short-term contractors are:
a.Favorable review of the security questionnaire form;
b.Favorable fingerprint results;
c.Favorable credit report, if required;5 and
d.Waiver request memorandum indicating both the position sensitivity/risk level and the duration of the appointment. The commensurate BI does not need to be initiated.
A badge may be issued following approval of the above waiver requirements and the badge will expire six months from the date of issuance. This process can only be used once for a short-term contractor in a twelve month period. This will ensure that any consecutive short-term appointments are subject to the full PFV-I identity proofing process.
For example, if a contractor employee requires daily access for a three or four-week period, this contractor would be cleared according to the above short-term requirements. However, if a second request is submitted for the same contractor employee within a twelve-month period for the purpose of extending the initial contract or for employment under a totally different contract for another three or four-week period, this contractor would now be considered "long-term" and must be cleared according to the long-term requirements as stated in this interim policy.

3. Intermittent Contractors:

An exception to the above-mentioned short-term requirements would be intermittent contractors.
a. For purposes of this policy, "intermittent" is defined as those contractor employees needing access to DOJ information systems and/or DOJ facilities or space for a maximum of one day per week, regardless of the duration of the required intermittent access. For example, the water delivery contractor that delivers water one time each week and is working on a one-year contract.
b. Contractors requiring intermittent access should follow the Department's escort policy. Please reference the August 11, 2004, and January 29, 2001, Department Security Officer policy memoranda that conveys the requirements for contractor facility escorted access.
c. Due to extenuating circumstances, if a component requests unescorted access or DOJ IT system access for an intermittent contractor, the same pre-employment background investigation waiver requirements that apply to short-term contractors are required.
d. If an intermittent contractor is approved for unescorted access, the contractor will only be issued a daily badge. The daily badge will be issued upon entrance into a DOJ facility or space and must be returned upon exiting the same facility or space.
e. If an intermittent contractor is approved for unescorted access, the approval will not exceed one year. If the intermittent contractor requires unescorted access beyond one year, the contractor will need to be re-approved each year.
4. An individual transferring from another department or agency shall not be re-adjudicated provided the individual has a current (within the last five years), favorably adjudicated BI meeting HSPD-12 and DOJ's BI requirements.
5.The DOJ's current escorted contractor policy remains unchanged by this acquisition notice.

NOTES:
1. FIPS 201 is available at: www.csrc.nist.gov/publications/fips/fips201 /FIPS-201-22505.pdf.
2. Under HSPD-12, long-term contractors are contractors having access to DOJ information systems and/or DOJ facilities or space for six months or longer. The PIV-I identity proofing process, including initiation and adjudication of the required background investiga-

tion, is required for all new long-term contractors regardless of whether it is the current practice to issue a badge. The second phase of HSPD-12 implementation (PIV-II) requires badge issuance to all affected long-term contractors.
3. For contractors in position sensitivity/risk levels above level 1, a favorable review of a credit check is required as part of the pre-appointment waiver package.
4. In order to avoid a delay in the hiring process, components should request an Advance NAC Report when initiating investigations to OPM. Per OPM 's instructions, to obtain an Advance NAC Report, a Code " 3" must be placed in block "B " of the " Agency Use Only " section of the investigative form. This report is available for all case types.
5. For contractors in position sensitivity/risk levels above level 1, a favorable review of a credit check is required as part of the pre-appointment waiver package.
(End of Clause)

DJAR-PGD-06-09 Reprogramming of Funds Notices to Congress for A-76 Competitions

Congressional Notification

Under the provisions of section 605(a) of the Department of Justice's appropriations act, an award in this procurement triggers a requirement that the Department notify congressional appropriations committees of actions resulting from the award which may include reorganization or contracting out of functions or activities presently performed by Federal employees.

An award in this procurement, and its implementation, are contingent upon satisfactory completion of the process required under section 605(a). After award, the Department will notify the source provider when this process has been satisfactorily completed and that implementation may begin. In the event that either cougressional committee expresses reservations, the Department may cancel the procurement and award, without charge or penalty. Because the contract/performance start date could be delayed or actually cancelled due to the reprogramming notice to Congress, it is understandable not to include the expected start date in A-76 solicitations. However, the lack of a contract/performance start date makes it difficult for potential source providers to propose realistic pricing in their proposals.

As a best practice, it is recommended that future solicitations for streamlined or standard competitions include a notice similar to the following sentences.
For pricing purposes only, offerors shall assume a contract/performance start date of XXXXXXXXXXX, which is the date it is assumed that the transition/phase-in period begins. The actual contract/performance start date may be different. (See the "Congressional Notification" term of the solicitation).
(End of Clause)

DJAR-PGD-07-10 Ensuring New Acquisitions Include Common Security Configurations

The following language is to be used in all appropriate solicitations and contracts.

(a) The provider of information technology shall certify applications are fully functional and operate correctly as intended on systems using the Federal Desktop Core Configuration (FDCC). This includes Internet Explorer 7 configured to operate on Windows XP and Vista (in Protected Mode on Vista). For the Windows XP settings, see: http://csrc.nist.gov/itsec/guidance_WinXP.html and for the Windows Vista settings, see: http://csrc.nist.gov/itsec/guidance_vista.html

(b) The standard installation, operation, maintenance, update, and/or patching of software shall not alter the configuration settings from the approved FDCC configuration. The information technology should also use the Windows Installer Service for installation to the default "program files" directory and should be able to silently install and uninstall.
(End of Clause)

DJAR-PGD-07-12 Maintaining Contractor Performance During a Pandamic or Other Emergency

Continuing Contract Performance During a Pandemic Influenza or other National Emergency

During a Pandemic or other emergency we understand that our contractor workforce will experience the same high levels of absenteeism as our federal employees. Although the Excusable Delays and Termination for Default clauses used in government contracts list epidemics and quarantine restrictions among the reasons to excuse delays in contract performance, we expect our contractors to make a reasonable effort to keep performance at an acceptable level during emergency periods.

The Office of Personnel Management (OPM) has provided guidance to federal managers and employees on the kinds of actions to be taken to ensure the continuity of operations during emergency periods. This guidance is also applicable to our contract workforce. Contractors are expected to have reasonable policies in place for continuing work performance, particularly those performing mission critical services, during a pandemic influenza or other emergency situation.

The types of actions a federal contractor should reasonably take to help ensure performance are:

Encourage employees to get inoculations or follow other preventive measures as advised by the public health service.
Contractors should cross-train workers as backup for all positions performing critical services. This is particularly important for work such as guard services where telework is not an option.
• Implement telework to the greatest extent possible in the workgroup so systems are in place to support successful remote work in an emergency.
• Communicate expectations to all employees regarding their roles and responsibilities in relation to remote work in the event of a pandemic health crisis or other emergency.
Establish communication processes to notify employees of activation of this plan.
• Integrate pandemic health crisis response expectations into telework agreements.
With the employee, assess requirements for working at home (supplies and equipment needed for an extended telework period). Security concerns should be considered in making equipment choices; agencies or contractors may wish to avoid use of employees' personal computers and provide them with PCs or laptops as appropriate.
• Determine how all employees who may telework will communicate with one another and with management to accomplish work. Practice telework regularly to ensure effectiveness.
• Make it clear that in emergency situations, employees must perform all duties assigned by management, even if they are outside usual or customary duties.
• Identify how time and attendance will be maintained.
It is the contractor's responsibility to advise the government contracting officer if they anticipate not being able to perform and to work with the Department to fill gaps as necessary. This means direct communication with the contracting officer or in his/her absence, another responsible person in the contracting office via telephone or email messages acknowledging the contractors notification.

The incumbent contractor is responsible for assisting the Department in estimating the adverse impacts of nonperformance and to work diligently with the Department to develop a strategy for maintaining the continuity of operations.
(End of Clause)

DJAR-PGD-08-04 Security of Systems and Data, Including Personally Identifiable Information

Security of Systems and Data, Including Personally Identifiable Data.

a. Systems Security
The work to be performed under this contract requires the handling of data that originated within the Department, data that the contractor manages or acquires for the Department, and/or data that is acquired in order to perform the contract and concerns Department programs or personnel.

For all systems handling such data, the contractor shall comply with all security requirements applicable to Department of Justice systems, including but not limited to all Executive Branch system security requirements (e.g., requirements imposed by OMB and NIST), DOJ IT Security Standards, and DOJ Order 2640.2E. The contractor shall provide DOJ access to and information regarding the contractor's systems when requested by the Department in connection with its efforts to ensure compliance with all such security requirements, and shall otherwise cooperate with the Department in such efforts. DOJ access shall include independent validation testing of controls, system penetration testing by DOJ, FISMA data reviews, and access by the DOJ Office of the Inspector General for its reviews.
The use of contractor-owned laptops or other media storage devices to process or store data covered by this clause is prohibited until the contractor provides a letter to the contracting officer (CO) certifying the following requirements:

1. Laptops must employ encryption using a NIST Federal Information Processing Standard (FIPS) 140-2 approved product;
2. The contractor must develop and implement a process to ensure that security and other applications software is kept up-to-date;
3. Mobile computing devices will utilize anti-viral software and a host-based firewall mechanism;
4. The contractor shall log all computer-readable data extracts from databases holding sensitive information and verify each extract including sensitive data has been erased within 90 days or its use is still required. All DOJ information is sensitive information unless designated as non-sensitive by the Department;
5. Contractor-owned removable media, such as removable hard drives, flash drives, CDs, and floppy disks, containing DOJ data, shall not be removed from DOJ facilities unless encrypted using a NIST FEPS 140-2 approved product;
6. When no longer needed, all removable media and laptop hard drives shall be processed (sanitized, degaussed, or destroyed) in accordance with security requirements applicable to DOJ;
7. Contracting firms shall keep an accurate inventory of devices used on DOJ contracts;
8. Rules of behavior must be signed by users. These rules shall address at a minimum: authorized and official use; prohibition against unauthorized users; and protection of sensitive data and personally identifiable information;
9. All DOJ data will be removed from contractor-owned laptops upon termination of contractor work. This removal must be accomplished in accordance with DOJ IT Security Standard requirements. Certification of data removal will be performed by the contractor's project manager and a letter confirming certification will be delivered to the CO within 15 days of termination of contractor work;

b. Data Security

By acceptance of, or performance on, this contract, the contractor agrees that with respect to the data identified in paragraph a. in the

event of any actual or suspected breach of such data (i.e., loss of control, compromise, unauthorized disclosure, access for an unauthorized purpose, or other unauthorized access, whether physical or electronic), the contractor will immediately (and in no event later than within one hour of discovery) report the breach to the DOJ CO and the contracting officer's technical representative (COTR). If the data breach occurs outside of regular business hours and/or neither the CO nor the COTR can be reached, the contractor shall call the DOJ Computer Emergency Readiness Team (DOJCERT) at 1-866-US4-CERT (1-866-874-2378) within one hour of discovery of the breach. The contractor shall also notify the CO as soon as possible during regular business hours.

c. Personally Identifiable Information Notification Requirement

The contractor further certifies that it has a security policy in place that contains procedures to promptly notify any individual whose personally identifiable information (as defined by OMB) was, or is reasonably believed to have been, breached. Any notification shall be coordinated with the Department, and shall not proceed until the Department has made a determination that notification would not impede a law enforcement investigation or jeopardize national security. The method and content of any notification by the contractor shall be coordinated with, and be subject to the approval of, the Department. The contractor assumes full responsibility for taking corrective action consistent with the Department's Data Breach Notification Procedures, which may include offering credit monitoring when appropriate.

d. Pass-through of Security Requirements to Subcontractors
The requirements set forth in Paragraphs a through c above, apply to all subcontractors who perform work in connection with this contract. For each subcontractor, the contractor must certify that it has required the subcontractor to adhere to all such requirements. Any breach by a subcontractor of any of the provisions set forth in this clause will be attributed to the contractor.

B. Information Resellers or Data Brokers

For contracts where the Department obtains PII from a contractor (such as an information reseller or data broker) but the contractor does not handle the data described in Section A of this guidance document, the following clause must be used:

Information Resellers or Data Brokers

Under this contract, the Department obtains personally identifiable information about individuals from the contractor. The contractor hereby certifies that it has a security policy in place which contains procedures to promptly notify any individual whose personally identifiable information (as defined by OMB) was, or is reasonably believed to have been, lost or acquired by an unauthorized person while the data is under the control of the contractor. In any case in which the data that was lost or improperly acquired reflects or consists of data that originated with the Department, or reflects sensitive law enforcement or national security interest in the data, the contractor shall notify the Department contracting officer so that the Department may determine whether notification would impede a law enforcement investigation or jeopardize national security. In such cases, the contractor shall not notify the individuals until it receives further instruction from the Department.
(End of Clause)

DJAR-PGD-08-05 Contractor Certification of Compliance with Federal Tax Requirements

Contractor Certification of Compliance with Federal Tax Requirements

By submitting a response to a solicitation or accepting a contract award, the contractor certifies that, to the best of its knowledge and belief, the contractor has filed all Federal tax returns required during the three years preceding the certification, has not been convicted of a criminal offense under the Internal Revenue Code of 1986, and has not, more than 90 days prior to certification, been notified of any unpaid Federal tax assessment for which the liability remains unsatisfied, unless the assessment is the subject of an installment agreement or offer in compromise that has been approved by the Internal Revenue Service and is not in default, or the assessment is the subject of a nonfrivolous administrative or judicial proceeding.
(End of Clause)

Section 4 - List of Attachments

This Section Is Intentionally Left Blank